Reliable and secret communication over adversarial multi-path networks

Qiaosheng (Eric) Zhang*[1] Swanand Kadhe*[2]
Mayank Bakshi[1] Sidharth Jaggi[1] Alex Sprintson[2]
[1]Institute of Network Coding, Chinese University of Hong Kong [2]Texas A& M University

***Abstract*—We consider the problem of communication over a *multi-path* network in the presence of a causal adversary. The limited-view causal adversary is able to eavesdrop on a subset of links and also jam on a potentially overlapping subset of links based on the current and past information. To ensure that the communication takes place reliably and secretly, resilient network codes with necessary redundancy are needed. We study two adversarial models – *additive* and *overwrite jamming* and we optionally assume *passive* feedback from decoder to encoder, *i.e.*, the encoder sees everything that the decoder sees. The problem assumes transmissions are in the *large alphabet* regime. For both jamming models, we find the capacity under four scenarios – reliability without feedback, reliability and secrecy without feedback, reliability with passive feedback, reliability and secrecy with passive feedback. We observe that, in comparison to the non-causal setting, the capacity with a causal adversary is strictly increased for a wide variety of parameter settings and present our intuition through several examples.**

***Index Terms*—adversary, jamming, secrecy, causal, feedback**

I. Introduction

Consider the following example of a communication problem. Alice wishes to wirelessly transmit a message m to receiver Bob by communicating over C different frequencies. Their communication is intercepted by a limited-view adversary Calvin who has his receiver tuned to subset Z_R of the frequencies, and can jam a potentially overlapping subset Z_W of frequencies by adding transmissions on them. Due to the nature of the channel, Calvin can only see the signal up to the current time to maliciously determine his jamming strategy for the current time instant. We wish to answer questions of the following form: "*Without knowing which frequencies Calvin is monitoring/jamming, what is the maximum communication rate at which Bob can decode Alice's message successfully, while keeping the message secret from Calvin?*". This example corresponds to a model in which Alice wishes to communicate reliably and secretly with Bob over a channel with an eavesdropper/additive jammer. A variant of the problem is when, additionally, Alice can also hear the channel outputs (she too is monitoring all C frequencies, and therefore has passive feedback). In this variant we wish to understand whether this knowledge can improve the best possible rate.

The work of Qiaosheng (Eric) Zhang, Mayank Bakshi and Sidharth Jaggi was partially supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08). The work of Alex Sprintson was partially supported by the NSF under grant CNS-0954153 and by the AFOSR under contract No. FA9550-13-1-0008.

* indicates equal contribution.

We model this problem as that of communication over a noiseless multi-path network consisting of C parallel links between the sender and the receiver. As mentioned above, the adversary Calvin can eavesdrop on a subset Z_R and jam on a subset Z_W. Subsets Z_{RW} , Z_{RO} and Z_{WO}[1] represent the links that Calvin can both eavesdrop on and jam, only eavesdrop on (but not jam) and only jam (but not eavesdrop on) respectively. In addition, the sizes of Z_{RW}, Z_{RO} and Z_{WO} are bounded from z_{rw}, z_{ro} and z_{wo}. The adversarial vector $\vec{z}$ = (z_{rw}, z_{ro}, z_{wo}) measures Calvin's power. Moreover, Calvin also knows the encoding and decoding schemes so that he may mimic Alice's behavior to confuse Bob. We consider a *causal* constraint on Calvin's behaviors, *i.e.*, Calvin can only use the knowledge of symbols up to the current time slot to decide his jamming strategy.

Related work

Reliable communication: The problem of reliable communication (with no secrecy constraints) against a malicious eavesdropping adversary has been well-studied in the past. The maximum possible rate has been characterized under various settings – both causal and non-causal. The non-causal setting is relatively well understood both in the classical error-correction setup [1]–[4] and the network error correction setting [5]–[8]. A key feature of these results is that in many of these models, Calvin can decrease the capacity by *twice* the number of links he controls, by "pushing" Alice's transmissions towards the "nearest plausible transmission", thereby inflicting "double-damage". This heuristic also suggests an intuitive scheme for Bob's decoder – try to detect as many corrupted links as possible and treat those as erasures – in this case Calvin's actions would only cause "single damage". Critically, Calvin's ability to cause double damage depends on his ability to be able to see the full transmission for each link in Z_R before determining the optimal jamming strategy for Z_W.

In contrast, in the causal setting, by using stochastic encoding, the adversary may not be able to predict some of the future symbols, which can then be used to detect the set Z_W. Causal adversaries for classical channel coding and network coding

[1]RW, RO, WO stand for "read and write", "read only" and "write only" respectively. In a wireless setting these sets may correspond to different physical constraints on Calvin's ability to eavesdrop on or jam certain frequencies. In distributed storage system setting these sets may correspond to Calvin having or read-or-write, read-only, or write-only permissions on different devices.

problems have also been well studied [9], [10]. In [11], the authors consider causal, omniscient adversaries for multicast networks, and characterize precise conditions under which any positive rate is achievable. Further, they also provide some upper and lower bounds on the rates. However, the question of characterizing the capacity in general networks containing malicious jammers remains open in the main.

Reliable and secret communication: The problem of *both* reliable *and* secure communication over a network has also received considerable attention in the literature. For reliable, secure communication, [12] characterize the capacity when $z_{ro} = z_{wo} = 0$. In [6], the authors consider another extreme when the set of edges that are eavesdropped and jammed are disjoint, *i.e.*, $z_{rw} = 0$. The capacity for a general $\vec{z} = (z_{rw}, z_{ro}, z_{wo})$ for a non-causal adversary with no feedback has been considered in a previous work [8] by the authors of this work.

Another model that is related to our setup is that of an adversarial wiretap (AWTP) channel [13], wherein the adversary can eavesdrop up to a given fraction of symbols sent over a channel, and can jam another (possibly intersecting) fraction of symbols based on what he eavesdrops. There are two key differences from our work: (i) the authors only consider the problem of additive jamming, and (ii) the capacity characterization is parametrized with "coarser granularity", in that instead of parametrizing the problem in terms of (z_{rw}, z_{ro}, z_{wo}), the authors parametrize it in terms of ($z_{rw} + z_{ro}, z_{rw} + z_{wo}$), *i.e.*, in terms of the total number of eavesdropped and jammed links.

Another problem that is closely related to ours is that of Secure Message Transmission (SMT) [14], [15]. Under SMT, a sender aims to communicate a message reliably and secretly to the receiver over multiple parallel links out of which a fraction of links are eavesdropped and another (possibly intersecting) fraction are jammed. There are a several differences from our model: (i) The SMT problem focusses on computing a lower bound on the number of links that are required for reliable and secret communication of one message symbol, and usually do not provide information-theoretically tight capacity characterizations, (ii) most schemes are multi-round, 2-way protocols where the receiver can (actively) talk to the sender (though some protocols are indeed 1-way), (iii) the problem parametrization is again in terms of $(z_{rw} + z_{ro}, z_{rw} + z_{wo})$.

Our contributions

We consider the problem of causal jamming with an optional secrecy requirement. Taking cue from our prior work [8], we consider a finer characterization of the adversary's power by classifying his controlled links into read-only, write-only, and read-and-write subsets. We examine this problem in two settings – additive and overwrite jamming. The motivation for an additive adversary comes from wireless networks, where, the adversary may add his own signal to the transmitted signal. On the other hand, the overwrite adversary models the adversarial action in a wired network, where the adversary is more likely to completely replace the true transmitted packets with fake packets of his choice. [2]

In the setting without feedback, Theorems 1-4 state the capacity when secrecy is not required. Theorems 5 and 6 state our results with secrecy requirement and also without feedback. When passive feedback is available to the encoder, we characterize the capacity in Theorems 7 and 8, and also consider secrecy in Theorems 9 and 10.

The rest of this paper is organized as follows. In Section II, we illustrate the role of causality in limiting the adversary's power by giving four examples. We formally define the problem in Section III and state our main results with short proof sketches in Section IV. The detailed proofs are presented in Appendices A-E.

II. Key ideas

The techniques used in this paper build upon the ideas introduced in [8], [12]. In this section, we present a short intuitive overview of some of these ideas via toy examples.

A. Ideas for achievability

1) Reed-Solomon codes: The application of Reed-Solomon codes [1] (or in fact, any MDS code) to network error-correction is well-studied. These are particularly useful when the parameters z_{rw}, z_{ro}, and z_{wo} correspond to a "strong adversary" that can choose both the set Z_W and the corrupted codewords in a "worst-case" manner.[3] If Bob were able to detect the set Z_W with high probability, this would allow him to treat the set Z_W as "erasures", thus enabling a rate of $C - z_w$ to be achievable – indeed, this is what some of the schemes we present attempt to do.[4]

2) Pairwise-hashing: When the adversary has limited knowledge of the transmitted codewords, in some settings a *pairwise-hashing* scheme is useful in detecting the set Z_W and enabling treating the corrupted set of links as erasures [12].The following example presents the main intuition here.

Example 1 (*Limited-view non-causal adversary [8]*)**.** Consider a network with three links L_1, L_2 and L_3, and an adversary Calvin that can both read and write on exactly one link, *i.e.*, $z_{rw} = 1$ and $z_{wo} = z_{ro} = 0$. Even though the zero-error capacity of this network is $C - 2z_w = 1$, we argue that in the vanishing error probability setup, the link Z_{RW} can be detected and the rate is $C - z_{rw} = 2$. The codeword sent on the link L_i consists of three parts – the i-th symbol from a $(3, 2)$ Reed-Solomon codeword U_i, a random key K_i, and hash values H_{i1}, H_{i2}, H_{i3} with $H_{ij} = h(K_i, U_j)$

[2]Notice that for a write only link, the overwrite adversary knows the output codewords while the additive adversary has no way to learn the output codewords.

[3]The simplest example of a strong adversary is an omniscient one, *i.e.*, when $z_r = C$. However, the exact parameter settings that correspond to a strong adversary depend on the flavour of the problem being considered, *e.g.* causal vs non-causal, overwrite vs additive etc.

[4]It is important here to make a distinction between zero error probability (*i.e.*, robustness to worst-case errors) and vanishing error probability requirements. In the former case one can use the Singleton bound [2] to see that the best achievable rate is $C - 2z_w$ regardless of what the adversary knows. However, the Singleton bound requires Calvin to know the entire transmission. Hence, in the latter setup, a higher rate may be achievable if the adversary has limited eavesdropping power.

for a suitably designed non-linear hash function $h(\cdot,\cdot)$. Upon receiving the codewords, Bob checks consistency within each pair of links (L_i, L_j) by verifying if the received values satisfy both $H_{ij} = h(K_i, U_j)$ and $H_{ji} = h(K_j, U_i)$. Without loss of generality, assume that Calvin choses $Z_{RW} = \{L_1\}$ (unknown to Alice and Bob) and corrupts $(U_1, K_1, H_{11}, H_{12}, H_{13})$. Note that since Calvin does not know the values of K_2 and K_3, it can be shown that the probability that he can satisfy the checks for H_{21} and H_{31} is small if he choses to change U_1. On the other hand, links L_2 and L_3 cross-verify all of their mutual hashes successfully, thus isolating L_1 as the corrupted link. As a result, Bob can successfully decode the message by treating U_1 as an erasure for the Reed-Solomon code. □

The scheme in the Example 1 exploits the adversary knowing only a subset of what the decoder sees. In the problems considered in this paper, the additional assumption of causality further limits his view and enables a higher rate. For example, in the three link network above, even if we permit the adversary to read all the links (*i.e.*, $z_{ro} = 2, z_{rw} = 1$), the fact that the adversary does not know the random keys K_1, K_2, K_3 while perturbing the selected U_i prevent him from being able to deterministically match the corresponding pairwise hashes. This allows the decoder to detect the corrupted link.

3) Adversary detection with passive feedback: We use a similar idea as above in the setting with passive feedback (*i.e.*, the encoder overhears all past symbols received by the decoder before transmitting the current symbol). In this case, the rate $C - z_w$ is possible for an even larger set of parameters by using a multi-round scheme that lets Bob detect the set of corrupted links.

Example 2 (*Adversary detection)***.** Consider a two link network with $z_{rw} = 1, z_{ro} = z_{wo} = 0$. Here, no positive rate is possible without feedback (*c.f.* Example 4). However, with passive feedback, a rate of 1 is possible. To see this, consider a two-round scheme. Alice first generates two independent and uniformly random keys K_1 and K_2. Next, for a message M, Alice transmits (M, K_1) and (M, K_2) on links L_1 and L_2 respectively in the first round. Now, Alice sees both the received codewords, say $(\hat{M}_1, \hat{K}_1)$ and $(\hat{M}_2, \hat{K}_2)$, and determines if any of the links were corrupted by Calvin. In the second round, Alice sends hash $H = (h(\hat{M}_1, \hat{K}_1), h(\hat{M}_2, \hat{K}_2))$ on all links that she determines to be uncorrupted in the first round, while sending uniformly random bits having the same length as H on the corrupted links. This lets Bob detect and ignore any link corrupted in the first round and decode the message from the uncorrupted link(s). Note that since Calvin sees only one link, he cannot ensure that the second round codeword on any link corrupted by him satisfies the hash equation.

The intuition is that the encoder can use his feedback to first determine which links have been corrupted by the adversary and then convey this information to the decoder by sending values consistent with the hash function only on the uncorrupted links (and inconsistent values on others).

4) Mixing keys for secrecy: In the setting where information theoretic secrecy is demanded in addition to reliability, we use standard one-time pad arguments that mix the message with random keys. Since the adversary can see up to z_r links, as long as the key rate is at least z_r, we show that the secrecy requirement is met. The error correcting code is chosen so that both the message and the key are decoded by the receiver. As a result, as long as the overall rate decreases by z_r, both secrecy and reliability are simultaneously met. [5]

5) Secret key extraction via passive feedback: A surprising effect of passive feedback is that it allows Alice and Bob to extract secret keys from corrupted links as long as the received codeword on the link is hidden from Calvin. This allows for simultaneous reliable and secret transmission at rates higher than that achievable by just mixing z_r random keys with the message. The following example of an *additive* adversary (*i.e.*, on Z_{WO} links, Calvin adds an error vector to the transmitted codeword without necessarily knowing what was sent by Alice) illustrates the key idea that enables achieving the rate $\min\{C - z_r, C - z_w\}$ in the additive setting.

Example 3 (*Secret key extraction)***.** Consider a two link network with $z_{ro} = z_{wo} = 1$. Here, no positive rate is possible for simultaneous reliable and secret transmission without feedback. However, with passive feedback, the following multi-round protocol achieves an asymptotic rate of 1. Let the message $M = M_1 M_2 \dots M_n$ be a length-n binary vector. The transmission is divided into three-stages. In the i-th round of the first stage, Alice generates a random bit K_j and sends $X_{1,j} = M_j$ on the first link and $X_{2,j} = M_j \oplus K_j$ on the second link. After each bit is received, Alice checks if any of the two links have been corrupted by Calvin. Let c be the first round where Calvin has corrupted one of the links, say link L_i, *i.e.*, $Y_{i,c} = X_{i,c} \oplus E_c$ for some E_c. Alice now starts the second stage of transmission. In each round $j = c+1, \dots, n+1$, Alice sends $X_{i,j} = K_j$ on the corrupted link L_i and $X_{i\oplus 1+1,j} = M_{j-1} + Y_{1,j-1}$ on the uncorrupted link. Note that since Calvin has revealed that $L_i \in Z_{WO}$, Alice knows that Calvin cannot infer the values of $Y_{i,j}$ as each $X_{i,j}$ is independent of $X_{i\oplus 1+1,1}, \dots, X_{i\oplus 1+1,n+1}$. Thus, in the second stage of transmission, $Y_{i,j}$ acts as a shared key for secret transmission on the uncorrupted link for the $(i+1)$-th round. Finally, in the third stage, Alice transmits the values of c and i by using the reliable transmission scheme (without secrecy) of Example 2.

B. Ideas for the converse

1) Cut-set bound: Since the adversary can corrupt z_w links, he can replace the codewords on the links in Z_W by uniformly random symbols independent of the original codewords. By a simple argument based on Fano's inequality, one can conclude that no rate higher than $C - z_w$ is possible if the error probability must vanish to 0.

2) A symmetrization argument [9]: A tighter converse than the above can be obtained when the adversary is "powerful enough". For example, in the setting without feedback, if the

[5]Note that decreasing the rate by z_r suffices even when Alice does not know the set of links corrupted by Calvin. Surprisingly, when Alice can learn the set of links corrupted by Calvin in previous rounds of a multi-round scheme, the secrecy capacity may be higher (as seen in Example 3)

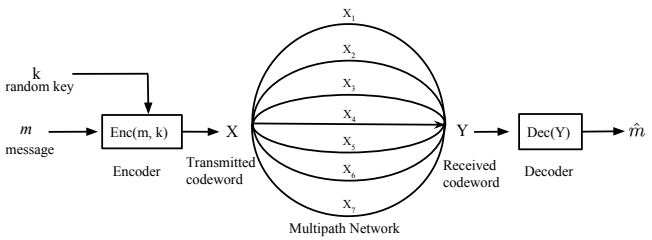

Fig. 1: System diagram for a multi-path network consisting of C parallel links ($C = 7$ in this example).

adversary can corrupt at least half of the links, no positive rate is possible. The argument here is similar to the Singleton Bound [2] and allows for stochastic encoding as well. The following example illustrates the idea.

Example 4 (*Symmetrization with a causal adversary*)**.** Consider a three link network under attack from a causal adversary with $z_{rw} = 2$ and $z_{wo} = z_{ro} = 0$. It is straightforward to see that the pairwise hashing scheme can be foiled by the adversary – he can ensure that the two links in Z_W satisfy each other's hashes and thus there is no reliable way for the decoder to determine the uncorrupted link. More generally, for any coding scheme, the adversary can follow a *symmetrization* strategy as follows. Suppose the encoder maps message m to codewords x_1, x_2, x_3 according to an encoder conditional probability distribution $p_{X_1,X_2,X_3|M}$.[6] The adversary first chooses a message m' uniformly at random from the set of possible messages and draws codewords x'_1, x'_2, x'_3 according to the conditional probability distribution $p_{X_1,X_2,X_3|M}\,(x'_1, x'_2, x'_3|m')$. Next, the adversary chooses Z_W to be either $\{L_1\}$ or $\{L_2, L_3\}$ with equal probability and replaces the codewords $(x_i : i \in Z_W)$ by $(x'_i : i \in Z_W)$. Now, from the decoder's point of view, given the received codewords y_1, y_2, y_3, the messages m and m' are equally likely. Thus, the decoder cannot reliably determine whether the true message is m or m' and as a result the error probability is bounded away from 0 for any code of positive rate. □

When feedback is present, an argument similar to the above holds, albeit for a smaller set of adversarial parameters. With feedback, since the code operates over multiple rounds, the adversary needs to be sufficiently powerful to be able to fool the decoder even when the encoder knows the received codewords on the links in Z_W.

III. Problem Statement

The multi-path network model and the encoding/decoding process are illustrated in Figure 1. In our setting, the multi-path network consists of C parallel, directed links L_1, L_2,...,L_C. For the equal link capacity network, each link is of unit capacity. For a general unequal link capacity network, the capacity of link L_i is denoted by u_i, $\forall i \in \{0, 1, \ldots, C\}$. The total capacity of a unequal link capacity network is defined as $\hat{C}$ bits per use, where $\hat{C} := \sum_{i=1}^{C} u_i$. In particular, the total capacity of the equal link capacity is C bits per use. We also optionally consider *passive feedback* available causally at the transmitter, *i.e.*, the transmitted overhears the received symbols at the decoder causally.

We begin by formally describing the encoder, decoder, and possible adversarial actions for a code for *block length* n, *i.e.*, for a code that operates over n time steps and r rounds ($r \leq n$ with $r = 1$ denoting the case without feedback). For simplicity, we focus on networks with equal link capacity and deal with the unequal link capacity case only informally.

In the following, matrices $X = [X^{(1)}X^{(2)}\ldots X^{(r)}]$ and $Y = [Y^{(1)}Y^{(2)}\ldots Y^{(r)}]$ respectively denote the collection of transmitted and received codewords across all links for all rounds. Here, $X^{(k)}$ (resp. $Y^{(k)}$) is a matrix whose i-th row $\vec{X}_i^{(k)}$ (resp. $\vec{Y}_i^{(k)}$) denotes the transmitted (resp. received) codeword on link L_i in the k-th round.

A. Encoder

The transmitter Alice encodes a nR-bit message m, where R stands for the message rate. The message m is assumed to be uniformly distributed from $\{0,1\}^{nR}$. To perform a stochastic encoding, a random key k, which is uniformed distributed from the finite field $\mathbb{F}_{2^t}$, is also generated by Alice.

In the first round, Alice encodes m into a collection of C n-length codewords $\vec{X}_1^{(1)}, \vec{X}_2^{(1)}, \ldots, \vec{X}_C^{(1)}$. In this case, the encoder function for the first round takes the form

$$\Psi_e^{(1)} : \{0,1\}^{Rn} \times \mathbb{F}_{2^t} \to \{0,1\}^{Cn^{(1)}}.$$

If no feedback is present, no further actions are performed by Alice. In this case, $n^{(1)} = n$.

If feedback is present, in each subsequent round k, Alice's codewords $\vec{X}_1^{(k)}, \vec{X}_2^{(k)}, \ldots, \vec{X}_C^{(k)}$ are each of length $n^{(k)}$ and are determined by the message m, the random key k, and the feedback from prior rounds $Y^{(1)}\ldots Y^{(k-1)}$. Formally, Alice's encoder for the i-th round takes the form

$$\Psi_e^{(k)} : \{0,1\}^{Rn} \times \mathbb{F}_{2^t} \times \prod_{j=1}^{k-1} \{0,1\}^{Cn^{(j)}} \to \{0,1\}^{Cn^{(k)}},$$

where, $\sum_{k=1}^{r} n^{(k)} = n$.

B. Decoder

The decoder Bob receives the code matrix Y, which may be different from X and outputs a reconstruction $\hat{m}$. The decoding function takes the form

$$\gamma_e(Y) : \{0,1\}^{nC} \to \{0,1\}^{nR}.$$

C. Adversary

Out of the C links of the multi-path network, the adversary Calvin is able to eavesdrop (but not jam) a subset Z_{RO} of size z_{ro}, jam (but not eavesdrop) a subset Z_{WO} of size z_{wo}, both eavesdrop and jam a subset Z_{RW} of z_{rw}. Calvin's power is measured by the adversarial vector $\vec{z} = (z_{rw}, z_{ro}, z_{wo})$. The encoding and decoding strategies are known to Calvin. However, the two end users do not know how Calvin chooses Z_{RO}, Z_{WO} and Z_{RW} in advance.

[6] Note that both a deterministic encoder as well as an encoder using pairwise hashing can be viewed as special cases under this formalism.

1) Additive and Overwrite Jamming: An additive jammer may induce additive bias on the transmitted codeword. Assume the codeword transmitted on L_i is $\overrightarrow{X}_i$ and the bias is $\overrightarrow{E}_i$, the received codeword would be $\overrightarrow{Y}_i = \overrightarrow{X}_i + \overrightarrow{E}_i$. On the other hand, an overwrite adversary can overwrite the transmitted codeword by its own one directly. If the codeword is $\overrightarrow{X}_i$ and the bias is $\overrightarrow{E}_i$, the received codeword will be $\overrightarrow{Y}_i = \overrightarrow{E}_i$.

2) Causal Adversary: We restrict the adversary to be *causal*, *i.e.*, the adversary is only allowed to jam the symbol of current time slot based on the observation of current and past time slots. More specifically, at any given time t, given a $C \times n$ code matrix X, the adversary can use the knowledge of only the first t symbols from rows in subset $Z_{RW} \cup Z_{RO}$ in order to jam the t-th symbols from the rows in $Z_{RW} \cup Z_{WO}$.

In contrast, a non-causal adversary [16] enjoys the full knowledge of all the symbols in the rows belonging to $Z_{RW} \cup Z_{RO}$ at all times. Obviously, the non-causal adversary has a stronger power and leads to a potentially lower rate.

3) Reliability and Security: Instead of a zero-error probability, we aim to achieve an ε-error probability. The communication is reliable if for any $\varepsilon > 0$, by choosing n large enough, there exists a code of block length n such that the error probability $P_e = Pr[m \neq \hat{m}] < \varepsilon$.

In terms of security, we aim to achieve the information-theoretically perfect secrecy. Assume the subset Calvin can eavesdrop is $Z_R = \{i_1, i_2, \cdots, i_{z_r}\}$ and the sub-codeword on Z_R links is $X_{Z_R} = [\overrightarrow{X}_{i_1}^T \overrightarrow{X}_{i_2}^T \cdots \overrightarrow{X}_{i_{z_r}}^T]^T$. To achieve security, the mutual-information between the message and Calvin's observation should be zero, i.e. $I(M; X_{Z_R}) = 0$.

IV. Main Results

In this section, we present the main results and sketch their proofs. The full proofs of the results can be found in Appendices B-E. We group our results into four parts – reliability without feedback, reliability and secrecy without feedback, reliability with feedback, as well as reliability and secrecy with feedback. For each of these cases, we discuss the additive jamming and the overwrite jamming separately. Finally, we give a "complete" characterization of the problem in Table I.

A. Reliability without feedback

For both additive and overwrite jammers, we obtain a two-part rate-region, i.e. *weak adversary regime* and *strong adversary regime*. The weak adversary regime for additive jamming is

$$\mathcal{Z}_{w,nf}^{add} = \{\vec{z} : z_{wo} + 2z_{rw} < C\},$$

whereas for overwrite jamming, the weak adversary regime is

$$\mathcal{Z}_{w,nf}^{ow} = \{\vec{z} : 2z_{wo} + 2z_{rw} < C\}.$$

The strong adversary regime equals the complement of the weak adversary regime. In the weak adversary regime, the achievability relies on erasure codes coupled with the pairwise-hashing scheme. The rate is limited to zero in the strong adversary regime.

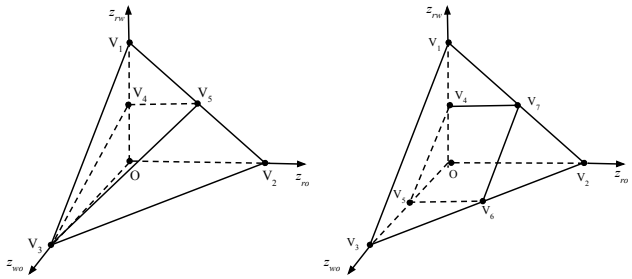

Fig. 2: The rate regions for additive and overwrite causal jamming adversaries (Theorem 1 and 2): for additive (resp. overwrite) jamming, the pentahedron $V_3OV_2V_5V_4$ (resp. $OV_4V_5V_2V_7V_6$) represents the weak adversary *regime, while the polyhedron $V_3V_4V_5V_1$ (resp. $V_1V_3V_5V_4V_7V_6$) represents the* strong adversary *regime.*

First we consider the scenario when reliable communication is the only objective. For equal and unequal link capacity networks, for any $\vec{z} = (z_{rw}, z_{ro}, z_{wo})$ such that $z_{rw} + z_{ro} + z_{wo} \leq C$, the maximum achievable reliable rates for additive and overwrite jamming are characterized in the following.

Theorem 1 (Additive jamming for equal link capacities)**.** *Under additive causal jamming, the maximum achievable reliable rate is*

$$R_j^{add}(C, \vec{z}) = \begin{cases} C - (z_{rw} + z_{wo}), & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{add}, \\ 0, & \text{otherwise}. \end{cases}$$

Theorem 2 (Overwrite jamming for equal link capacities)**.** *Under overwrite causal jamming, the maximum achievable reliable rate is*

$$R_j^{ow}(C, \vec{z}) = \begin{cases} C - (z_{rw} + z_{wo}), & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{ow}, \\ 0, & \text{otherwise}. \end{cases}$$

For additive jamming and overwrite jamming, the two-part rate-regions are slightly different though the expressions are similar. Note that, regardless of the coding scheme, the best rate that we can hope for is $C - z_w$ since the adversary can corrupt any z_w links. In the weak adversary regime, the best rate $C - z_w$ is indeed achievable. To achieve it, the encoder would use an erasure code to encode the message and apply the pairwise-hashing scheme to help detect errors. The decoder detects the corrupted links first (which are regarded as erasures) and then the message will be retrieved from the sub-codewords carried by the uncorrupted links.

However, no coding scheme (including pairwise-hashing) works for the strong adversary regime. The adversary can always adopt a "symmetrization" strategy so that the decoder is unable to distinguish the correct message and the fake message. The proof of the converse relies on an argument based on the Singleton bound [2] that we present in Appendix B.

Unequal link capacities: To incur maximum damage, the adversary may choose links with highest sum-rate to attack. We define the the total capacity of any subset of size w links as U_w. Different choice of the subsets may incur different values of U_w. Typically, the notation $(U_w)_{max}$ is used to denote the maximum value of U_w, i.e. the largest sum-capacity of

all possible subsets of size w. Similar to the situation with equal link capacities, the main idea is also encoding by erasure codes as well as adopting "pairwise-hashing" scheme to detect adversarial attacks. However, the only difference is that the maximum rate depends on Calvin's ability to corrupt the links with largest sum-capacities.

Theorem 3 (Additive jamming for unequal link capacities)**.** *Under additive causal jamming, the maximum achievable reliable rate is*

$$R_j^{add}(\hat{C},\vec{z}) = \begin{cases} \hat{C} - (U_{(z_{rw}+z_{wo})})_{max}, & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{add} \\ 0, & \text{otherwise}. \end{cases}$$

Theorem 4 (Overwrite jamming and unequal link capacities)**.** *Under overwrite causal jamming, the maximum achievable reliable rate is*

$$R_j^{ow}(\hat{C},\vec{z}) = \begin{cases} \hat{C} - (U_{(z_{rw}+z_{wo})})_{max}, & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{ow}, \\ 0, & \text{otherwise}. \end{cases}$$

B. Reliability and secrecy without feedback

In this section, we consider the scenario wherein Calvin tries to learn some information about Alice's message from the links he eavesdrops. Besides reliable communication, we also want to prevent Calvin from gaining any information about the message. For this, we consider information-theoretically perfect secrecy, which requires that $I(M; X_{Z_R}) = 0$, where X_{Z_R} is the sub-codeword transmitted on the links in Z_R. In the following, we characterize the reliable and secure rate region in the equal link capacity case for the causal adversary.

Theorem 5 (Additive, causal jamming with secrecy, equal link capacities)**.** *Under additive causal jamming, the maximum achievable reliable and secret rate is*

$$R_{j,s}^{add}(\vec{z}) = \begin{cases} (C - (z_{wo} + z_{ro} + 2z_{rw}))^+ & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{add}, \\ 0 & \text{otherwise}, \end{cases}$$

where $(x)^+$ *is defined as* $(x)^+ = \max\{0, x\}$.

Theorem 6 (Overwrite, causal jamming with secrecy, equal link capacities)**.** *Under overwrite causal jamming, the maximum achievable reliable and secret rate is*

$$R_{j,s}^{ow}(\vec{z}) = \begin{cases} (C - (z_{wo} + z_{ro} + 2z_{rw}))^+ & \text{if } \vec{z} \in \mathcal{Z}_{w,nf}^{ow}, \\ 0 & \text{otherwise}, \end{cases}$$

where $(x)^+$ *is defined as* $(x)^+ = \max\{0, x\}$.

The converse for the weak adversary regime (for both additive and overwrite jamming) follows from the standard information-theoretic inequalities, where we use the secrecy condition that any subset of $z_r = (z_{rw} + z_{ro})$ links cannot carry any meaningful information. In the achievable scheme, Alice needs to *mix* her message with z_r random keys and then use the reliable encoding scheme consisting of pairwise hashing and erasure coding. For the strong adversary regime, the converse is based on the Singleton-type arguments similar to the only reliability case. We present the detail proof in Appendix C.

C. Reliability with passive feedback

In this section, we examine the effect of passive feedback on the capacity under jamming for both additive and overwrite settings. For both these cases, the parameter space again decomposes into two parts - the *weak adversary regime* and *strong adversary regime*.

The main idea for achievability of the claimed rate in the weak adversary regime is to use a two-round code. The first round involves sending a code that can handle up to $z_{rw} + z_{wo}$ erasures. At the end of the first round, Alice sees the codewords received by Bob and determines the links which have been corrupted. In the next round, Alice sends a random hash of all the received codewords by Bob on the uncorrupted links from first round. Bob can then check the received values from the second round to determine the links where the hash values do not match the received codeword and treat those links as erasures.

The above scheme works as long as there is at least one link whose output is not seen by Calvin. This corresponds exactly to the condition for the weak adversary in the following theorems. If Calvin is able to see the output of all the links, he is as powerful as Alice and feedback no longer helps.

Theorem 7 (Additive Jamming with Causal Feedback)**.** *Under an additive jamming with causal feedback, the capacity is*

$$R_{j,f}^{add} = \begin{cases} 0 & \text{if } z_r = C \text{ and } C \leq 2z_w \\ C - z_w & \text{otherwise} \end{cases}$$

Theorem 8 (Overwrite Jamming with Causal Feedback)**.** *Under an overwrite jamming with causal feedback, the capacity is*

$$R_{j,f}^{ow} = \begin{cases} \max\{C - 2z_w, 0\} & \text{if } z_{ro} + z_{rw} + z_{wo} = C \\ C - z_w & \text{otherwise} \end{cases}$$

We present the detailed proof in Appendix D.

D. Reliability and secrecy with passive feedback

The schemes for secrecy are similar to that for only reliability. The idea here is to mix appropriate number of random keys so as to prevent Calvin from inferring meaningful information. The protocols operate over multiple rounds. For overwrite jamming, Alice begins with mixing z_r number of keys. If Calvin corrupts a link, Alice detects the corrupted link through passive feedback and stops using that link from the next round. After Calvin corrupts z_{wo} links, for any more link that he corrupts, Alice reduces the number of random keys by one. In essence, Alice does not send any data on (up to) z_w links that Calvin corrupts, and uses z_{ro} number of random keys. Roughly speaking, the scheme is secure because Calvin does not observe anything on z_{rw} links, and z_{ro} number of random keys protect the data on z_{ro} links that Calvin can only eavesdrop.

For additive jamming, Alice leverages the fact that Calvin cannot observe data on z_{wo} links. Here, when Calvin corrupts a link, she starts sending random symbols on that link. The idea is that, even after Calvin corrupts the symbols by adding any noise of his choice, z_{wo} of them can be used as keys for

TABLE I: The table gives expressions for the information-theoretically optimal rate regions in each scenario. The yellow cells refer to the main results presented in [8]. The new results presented in this paper are shown in red cells. We use $(x)^+$ to represent $\max\{0, x\}$.

Model		regime	reliability	reliability & secrecy
Non-causal	additive	$z_{ro} + z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{ro} + z_{wo} + 2z_{rw} \geq C$	$(C - 2z_{rw} - z_{wo})^+$ $(\hat{C} - (\Lambda_{2z_{rw}+z_{wo}})_{max})^+$	0
	overwrite	$z_{ro} + 2z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{ro} + 2z_{wo} + 2z_{rw} \geq C$	$(C - 2z_{rw} - 2z_{wo})^+$ $(\hat{C} - (\Lambda_{2z_{rw}+2z_{wo}})_{max})^+$	0
Causal w/o feedback	additive	$z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{wo} + 2z_{rw} \geq C$	0	0
	overwrite	$2z_{wo} + 2z_{rw} < C$	$C - (z_{rw} + z_{wo})$ $\hat{C} - (\Lambda_{z_{rw}+z_{wo}})_{max}$	$(C - z_{ro} - z_{wo} - 2z_{rw})^+$
		$z_{wo} + 2z_{rw} \geq C$	0	0
Causal with passive feedback	additive	$\{z_r = C \text{ and } 2z_w < C\} \bigcup \{z_r < C\}$ $z_r = C \text{ and } 2z_w \geq C$	$C - (z_{rw} + z_{wo})$ 0	$\min\{C - z_r, C - z_w\}$ 0
	overwrite	$z_{ro} + z_{wo} + z_{rw} < C$ $z_{ro} + z_{wo} + z_{rw} = C$	$C - (z_{rw} + z_{wo})$ $(C - 2z_{wo} - 2z_{rw})^+$	$(C - z_{ro} - z_{wo} - z_{rw})^+$ 0

the next round. This limits the number of explicit keys to be mixed and enhances the rate.

The following theorem formally states the capacity expressions for the above settings.

Theorem 9 (Secrecy capacity with Causal Feedback, Additive Jamming)**.** When causal passive feedback available to the encoder, the capacity for simultaneous reliability and secrecy is given by

$$R_{j,f}^{add} = \begin{cases} (C - z_r)^+ & \text{if } z_r \geq z_w \\ (C - z_w)^+ & \text{if } z_w > z_r \end{cases}$$

Theorem 10 (Secrecy capacity with Causal Feedback, Overwrite Jamming)**.** When causal passive feedback available to the encoder, the capacity for simultaneous reliability and secrecy is given by

$$R_{j,f}^{ow} = (C - z_{ro} - z_{wo} - z_{rw})^+.$$

As earlier, we give the full proof in Appendix E.

REFERENCES

[1] I. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960. [Online]. Available: http://dx.doi.org/10.1137/0108018

[2] R. C. Singleton, "Maximum distance q -nary codes," *Information Theory, IEEE Transactions on*, vol. 10, no. 2, pp. 116–118, Apr 1964.

[3] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Proc. EUROCRYPT 84 workshop on Advances in cryptology: theory and applicationof cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 33–51.

[4] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.

[5] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," in *Proceedings of International Symposium in Information Theory (ISIT 2005)*, Adelaide, Australia, 2005, pp. 1455–1459.

[6] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network codes resilient to jamming and eavesdropping," in *Proc. Workshop on Network Coding Theory and Applications*, Toronto, Canada, Jun. 9–11 2010.

[7] S. Jaggi and M. Langberg, "Network security," in *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, Eds. Academic Press, 2012.

[8] Q. Zhang, S. Kadhe, M. Bakshi, S. Jaggi, and A. Sprintson, "Talking reliably, secretly, and efficiently: A "complete" characterization," in *Information Theory Workshop (ITW), 2015 IEEE*. IEEE, 2015, pp. 1–5.

[9] B. Dey, S. Jaggi, and M. Langberg, "Codes against online adversaries, part i: Large alphabets," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3304–3316, 2013.

[10] L. Nutman and M. Langberg, "Adversarial models and resilient schemes for network coding," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, Canada, Jul. 6–11, 2008, pp. 171–175.

[11] O. Kosut and L.-W. Kao, "On generalized active attacks by causal adversaries in networks," in *Information Theory Workshop (ITW), 2014 IEEE*. IEEE, 2014, pp. 247–251.

[12] S. Jaggi, "Design and analysis of network codes," Dissertation, California Institute of Technology, 2005.

[13] P. Wang and R. Safavi-Naini, "An efficient code for adversarial wiretap channel," in *Information Theory Workshop (ITW), 2014 IEEE*. IEEE, 2014, pp. 40–44.

[14] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *Journal of the Association for Computing Machinery*, vol. 40, no. 1, pp. 17–47, January 1993.

[15] A. Patra, A. Choudhury, C. Pandu Rangan, and K. Srinathan, "Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality," *International Journal of Applied Cryptography*, vol. 2, no. 2, pp. 159–197, 2010.

[16] Q. Zhang, S. Kadhe, M. Bakshi, S. Jaggi, and A. Sprintson, "Talking reliably, secretly, and efficiently: A complete characterization," Accepted for ITW 2015. Long version available at http://personal.ie.cuhk.edu.hk/~mayank/ZhangKBJS14.pdf.

APPENDIX A
AUXILIARY LEMMAS

Definition 1 (Matrix-hashing)**.** *For any $N \times N$ square matrix A and vector $\vec{\rho}$ of length N, the matrix-hash $h(A, \vec{\rho})$ is defined as $\vec{\theta} = A\vec{\rho}$, where $\vec{\theta}$ is also of length N.*

Lemma 1. *Let q be a prime power. Suppose the $N \times N$ matrix A is uniformly distributed over $\mathbb{F}_q^{N\times N}$ and the length-N non-zero vector $\vec{\rho}$ is also uniformly distributed over $F_q^N \backslash \{0\}$. Let $\hat{A}$ be a random matrix independent from A and $\vec{\rho}$ be distributed over $\mathbb{F}_q^{N\times N}$ with some distribution $P_{\hat{A}}(\cdot)$. Then for any $\vec{\rho}$ not equal to zero,*

$$\Pr_{\hat{A},A,\rho}[\hat{A}\vec{\rho} = A\vec{\rho}] \leq \frac{1}{q}.$$

Proof: The matrices A and $\hat{A}$ are uniformly distributed over finite field $\mathbb{F}_q$, and they are also independent from each other. Therefore the difference of the two matrices $\hat{A} - A$ should also be a matrix which is uniformly distributed over $\mathbb{F}_q^{N\times N}$. We use the fact that a random matrix over $\mathbb{F}_q$ is non-invertible with probability at most $\frac{1}{q}$. Since $\vec{\rho}$ is non-zero, the equation $(\hat{A} - A)\vec{\rho} = 0$ only if the matrix $\hat{A} - A$ is non-invertible. Therefore we conclude that

$$\Pr_{\hat{A},A,\rho}[\hat{A}\vec{\rho} = A\vec{\rho}] = \Pr_{\hat{A},A,\rho}[(\hat{A} - A)\vec{\rho} = 0] \leq \frac{1}{q}.$$

Lemma 2. *Let q be a prime power and suppose the $N \times N$ matrix A is uniformly distributed over $\mathbb{F}_q^{N\times N}$. Let $\hat{\theta}$ be a random length-N vector distributed over $\mathbb{F}_q^N$ independently from A and according to an arbitrary distribution $P_{\hat{\theta}}^{\vec{\rho}}(\cdot)$. Then for any non-zero length-N vector $\vec{\rho}$,*

$$\Pr_{A,\hat{\theta}}[A\vec{\rho} = \vec{\hat{\theta}}] \leq \frac{N}{q}.$$

Proof: Each row $\vec{A_i}$ of matrix A is uniformly distributed over the finite field $\mathbb{F}_q^N$ and independent from vector $\vec{\rho}$ by the definition of matrix A. For every i *s.t.* $1 \leq i \leq N$, $\vec{\theta_i} = \vec{A_i}\vec{\rho}$ is also uniformly distributed over $\mathbb{F}_q$. Therefore, the vector $\vec{\theta}$ is uniformly distributed over $\mathbb{F}_q^N$ and for each i,

$$\Pr_{A,\hat{\theta}}[\vec{\theta_i} = \vec{\hat{\theta}_i}] \leq \frac{1}{q}$$

by Schwartz-Zipple Lemma. By applying the Union bound, we conclude that

$$\Pr_{A,\hat{\theta}}[A\vec{\rho} = \vec{\hat{\theta}}] = \Pr_{A,\hat{\theta}}[\vec{\theta} = \vec{\hat{\theta}}] \leq \frac{N}{q}.$$

APPENDIX B
PROOFS FOR RELIABLITY WITHOUT FEEDBACK

In the presence of a causal adversary, a two-part rate-region is presented in Section IV. In this Appendix we provide supporting proofs for Theorems 1 and 2, which provide the claimed characterizations of the two-part rate-regions for additive jamming and overwrite jamming.

A. Proof of Theorem 1

1) Achievability for weak adversary regime: Since the adversary can only jam in a causal manner, a *pairwise-hashing scheme* is helpful to achieve the best rate for the weak adversary regime.

Encoder: The encoder operates over a finite field $\mathbb{F}_q$, where $q = 2^b$ and we set $b = \log(nC)$ for equal link capacities while $b = \log(n\hat{C})$ for unequal link capacities. Choose N such that $N^2 + N(C+1) = \frac{n}{b}$. The codeword consists of C vectors $\overrightarrow{X}_1, \overrightarrow{X}_2, \ldots, \overrightarrow{X}_C$, each of length $N^2 + N(C+1)$ over the finite field $\mathbb{F}_q$. Each $\overrightarrow{X}_i$ is of the form

$$\overrightarrow{X}_i = [\overrightarrow{U}_i \overrightarrow{K}_i \vec{h}_{i1}, \vec{h}_{i2}, ..., \vec{h}_{iC}].$$

Here, $\overrightarrow{U}_i$ is such that $\overrightarrow{U}_1, \overrightarrow{U}_2, \ldots, \overrightarrow{U}_C$ together form the codeword corresponding to the length-nR_j^{add} bit message m using a Reed-Solomon code of length C and rate $C - z_{rw} - z_{wo}$ over the finite field $\mathbb{F}_q^{N^2}$. $\overrightarrow{K}_i$ is the hash key generated for each row. The value of hash function $h(\overrightarrow{U}_j, \overrightarrow{K}_i)$ is defined as $\vec{h}_{ij}$. For each link L_i, the encoder also appends C pairwise hashes $\vec{h}_{i1}, \vec{h}_{i2}, ..., \vec{h}_{iC}$ corresponding to the C links.

Hash Function: The idea of *Matrix-hashing* (see Lemma 1 in Appendix A) is used for the hash function. Notice that the randomly generated hash keys are of size N and each length-N^2 payload $\overrightarrow{U}_i$ can be rearranged as a $N \times N$ matrix D_i. We pad auxiliary bits before the packets if a square matrix cannot be formed. The hashes $\vec{h}_{ij}$ is obtained from the hash function $h(\overrightarrow{U}_j, \overrightarrow{K}_i) = D_j \overrightarrow{K}_i$.

Decoder: After transmission, the received packet of the i-th link L_i is of the form

$$\overrightarrow{Y}_i = [\overrightarrow{U'}_i \; \vec{K}_i'^T \; \vec{h}_{i1}'^T \; \vec{h}_{i2}'^T \cdots \vec{h}_{iC}'^T].$$

For each i, j, link L_i and L_j are consistent if and only if $\vec{h}'_{ij} = h(\overrightarrow{U'}_j, \overrightarrow{K'}_i)$ and $\vec{h}'_{ji} = h(\overrightarrow{U'}_i, \overrightarrow{K'}_j)$. In particular, link L_i is called self-consistent if and only if $\vec{h}'_{ii} = h(\overrightarrow{U'}_i, \overrightarrow{K'}_i)$.

The decoder Bob first removes the links that belong to Z_{WO} by checking self-consistency. Then Bob constructs an undirected graph with C vertices and for $\forall i, j$, he connects the two vertices v_i and v_j if L_i and L_j are consistent. To detect the uncorrupted links, Bob adopts a *"finding largest clique"*[7] strategy, i.e., a link is assumed to be uncorrupted if its corresponding vertex belongs to the largest clique. Finally, Bob decodes the message from the $C - z_w$ uncorrupted links by Reed-Solomon code.

Analysis: Before transmission, any two links are consistent and the clique formed by Alice is of size C. After adversarial corruption, the size of clique formed by Alice (*correct clique*) is of size at least $C - z_w$. On the other hand, Calvin may mimic the behavior of Alice and and attempt to form a fake clique that is as large as possible. For any two links belonging to Z_{RW}, Calvin is able to make them consistent since he can modify the payload first, and then compute matching hashes to insert. However, if link L_i belongs to Z_{RW} and link L_j belongs to Z_{RO}, Calvin cannot induce consistency

[7]The method, comes up in [5], is not an NP complete problem.

since $\vec{h}'_{ji} \neq h(\overrightarrow{U}'_i, \overrightarrow{K}'_j)$ with high probability. This is because with causality, Calvin doesn't have the ability to observe $\overrightarrow{K}_j$ and $\vec{h}_{ji}$ when modifying $\overrightarrow{U}_i$. In this scenario, the probability that Calvin can induce $\vec{h}'_{ji} = h(\overrightarrow{U}'_i, \overrightarrow{K}'_j)$ is at most $\frac{1}{q}$ over finite field $\mathbb{F}_q$ (see Lemma 1 in Appendix A). We would like to make q larger, *i.e.*, enlarge the size of the packet, to reduce the error probability.

In conclusion, Calvin is able to form a fake clique of size at most z_{rw}. If Bob wishes to figure out the uncorrupted links by finding largest clique, the size of correct clique should be larger than the fake clique, i.e. $C - z_w > z_{rw}$. Therefore we derive the condition for our weak adversary regime, which is $z_{wo} + 2z_{rw} < C$, and the rate $R = C - z_{rw} - z_{wo}$ can be achieved. [8]

2) Converse for weak adversary regime: Irrespective of the encoding/decoding scheme, Calvin can always add uniformly random noise to any z_w links. No information can be recovered from the z_{wo} links and thus no rate higher than $C - z_w$ is possible.

3) Converse for strong adversary regime: In the strong adversary regime ($z_{wo}+2z_{rw} \geq C$), we prove that no reliable communication is possible no matter which encoding scheme Alice will use. To confuse Bob, the causal adversary Calvin will always adopt the following *"symmetrization"* strategy: (a) corrupt the last z_{wo} (*resp.* $z_{wo}+1$) links by adding random noise if $C - z_{wo}$ is even (*resp.* odd), and (b) "attack" either the top half or the bottom half of the remaining $C' = C - z_{wo}$ (*resp.* $C' = C - z_{wo} - 1$) links, where the "attack" is defined below. This is a viable jamming strategy for Calvin since $z_{rw} \geq (C - z_{wo})/2$ in the strong adversary regime. The specific attack Calvin chooses is to pick a message m' first and substitute the original codewords belong to Z_{RW} by the codewords corresponding to m'. In this way, Bob has no idea whether m or m' was transmitted.

We assume the message M is uniformly distributed from the message set $\mathcal{M}$, denoted by U_M. Let X_R be the random variable of the codeword. Moreover, $X_R(m)$ is used to represent the random variable of the codeword conditioned on message m. The event $\Gamma(m, k, m', k')$ stands for the scenario when Alice chooses a message m and a random key k while Calvin chooses a message m' and a random key k'. We can show that the probability of the event $\Gamma(m, k, m', k')$ and the event $\Gamma(m', k', m, k)$ are exactly the same.

$$\begin{aligned} &Pr[\Gamma(m, k, m', k')] \\ =&U_M(m)P_{X_R(m)}(X)U_M(m')P_{X_R(m')}(X') \\ =&U_M(m')P_{X_R(m')}(X')U_M(m)P_{X_R(m)}(X) \\ =&Pr[\Gamma(m', k', m, k)] \end{aligned}$$

Let $P_y(m, k, m', k')$ and $P_y(m', k', m, k)$ denote the distributions of the received codeword conditioned on the events $\Gamma(m, k, m', k')$ and $\Gamma(m', k', m, k)$ respectively. Given the event $\Gamma(m, k, m', k')$, the received codeword would be either

$$[\overrightarrow{X}_1, ..., \overrightarrow{X}_{\frac{C'}{2}}, \overrightarrow{X}'_{\frac{C'}{2}+1}, ..., \overrightarrow{X}'_{C'}, \overrightarrow{N}_{C'+1}, ..., \overrightarrow{N}_C]$$

or

$$[\overrightarrow{X}'_1, ..., \overrightarrow{X}'_{\frac{C'}{2}}, \overrightarrow{X}_{\frac{C'}{2}+1}, ..., \overrightarrow{X}_{C'}, \overrightarrow{N}_{C'+1}, ..., \overrightarrow{N}_C]$$

with equal probability. The same distribution of the codeword will be received when the event $\Gamma(m', k', m, k)$ happens. We conclude that the distributions $P_y(m, k, m', k')$ and $P_y(m', k', m, k)$ are exactly the same. Therefore Bob cannot distinguish the events $\Gamma(m, k, m', k')$ and $\Gamma(m', k', m, k)$ when decoding, and thus has no idea whether m or m' are transmitted. The error probability is

$$\Pr(error) = \frac{1}{2}(1 - \frac{1}{2^{nR_j^{add}}})$$

if Bob uses an optimal maximum-likelihood decoder (the term $1 - \frac{1}{2^{nR_j^{add}}}$ is due to the "small" probability that the message m' Calvin chooses to use to confuse Bob happens to actually match Alice's message m).

B. Proof of Theorem 2

1) Achievability for the weak adversary regime: The pairwise-hashing scheme also works for the overwrite jammer. The encoding scheme here is the same as that in the additive case. We briefly describe it below for completeness. As earlier, we first generate a payload $\overrightarrow{U}_i$ for each link L_i using a Reed-Solomon code. Next, we append the hash key and pairwise hashes to the the payload to obtain the codeword $\overrightarrow{X}_i = [\overrightarrow{U}_i \overrightarrow{K}_i \vec{h}_{i1}, \vec{h}_{i2}, ..., \vec{h}_{iC}]$. After transmission, the received packet is denoted by $\overrightarrow{Y}_i = [\overrightarrow{U}'_i \; \vec{K}_i{}'^T \; \vec{h}'^T_{i1} \; \vec{h}'^T_{i2} \cdots \vec{h}'^T_{iC}]$. As in the additive case, the decoder forms an undirected decoding graph with C nodes and connects two vertices v_i and v_j if L_i and L_j are consistent. Finally, the decoder finds the largest clique in the decoding graph to determine the set of uncorrupted links. Although the same encoding strategy is applied, a different rate-regime is obtained since the overwrite jammer is slightly stronger than the additive one.

Analysis: After transmission, the size of the *correct clique* is at least $C - z_w$ since Calvin doesn't have privilege to jam on these links. At the same time, Calvin is able to induce a *fake clique* of size no larger than $z_{rw} + z_{wo}$. This is because on the links that belong to Z_{RW} and Z_{WO}, Calvin can overwrite the payloads first and then overwrite the hash vectors with appropriately computed replacements.. Therefore the corresponding vertices will form a clique of size $z_{rw}+z_{wo}$. Notice that from the receiver's perspective, the subset Z_{RW} is equivalent to Z_{WO} with overwrite jamming. With additive jamming, we have proved the fake clique that Calvin may induce is of size z_{rw}. Therefore as long as $z_{rw}+z_{wo} < C-z_w$, the rate $R = C - z_w$ is achievable.

2) Converse for weak adversary regime: Irrespective of the encoding/decoding scheme, Calvin can always arbitrarily choose a subset Z_W and overwrite these links by adding noises. As a result, at most $C - z_w$ links can carry useful information and thus the maximum rate is at most $C - z_w$.

[8] Notice that the links belong to Z_{WO} are also detectable by simply checking the self-consistency. We claim a link belongs to Z_{WO} if it is not self-consistent. However, this process is not necessary since we can detect the uncorrupted links by finding the largest clique.

3) Converse for strong adversary regime: The condition for strong adversary regime is $z_{rw} + z_{wo} \geq C/2$ with overwrite jamming. In this regime, the adversary is able to jam at least half of the C links and may perform a similar *"symmetrization"* strategy. Irrespective of the coding scheme, Calvin will (a) first pick a message m' and a key k' randomly to obtain the corresponding codeword X', (b) then attack either the top half or the bottom half (If C is odd, Calvin will first "erase" one link by overwrite it with a zero packet). In this case, the messages m and m' are perfectly symmetric so that Bob is unable to distinguish them.

If the event $\Gamma(m, k, m', k')$ happens, the received codeword would be either

$$[\overrightarrow{X}_1, ..., \overrightarrow{X}_{\frac{C}{2}}, \overrightarrow{X}'_{\frac{C}{2}+1}, ..., \overrightarrow{X}'_C]$$

or

$$[\overrightarrow{X}'_1, ..., \overrightarrow{X}'_{\frac{C}{2}}, \overrightarrow{X}_{\frac{C}{2}+1}, ..., \overrightarrow{X}_C]$$

with equal probability. Meanwhile, the received codeword has the same distribution when the event $\Gamma(m', k', m, k)$ happens. Therefore the distributions $P_y(m, k, m', k')$ and $P_y(m', k', m, k)$ are also the same and Bob is unable to decide which message is transmitted. The error probability is equal to $\Pr(error) = \frac{1}{2}(1 - \frac{1}{2^{nR_j^{ow}}})$ if a random decision is made.

APPENDIX C
PROOFS FOR RELIABLITY AND SECRECY WITHOUT FEEDBACK

A. Proof of Theorem 5

1) Weak adversary Regime:

Converse: Consider the following strategy for Calvin. First, on the links in Z_W he adds uniformly random noise that is independent of the codewords on other links. Next, he eavesdrops on all Z_R links. We show that, using standard information-theoretic inequalities, that it is not possible for Alice to reliably and secretly transmit at any rate more than $C - z_w - z_r$. Notice that Calvin can jam any z_w links and can eavesdrop any z_r links. Consider a code of length n that achieves an error probability ϵ_n and achieves perfect secrecy. The following set of inequalities follow.

$$\begin{aligned}
H(M) &= H(M|Y) + I(M;Y) \\
&\overset{(a)}{\leq} n\epsilon_n + I(M;Y) \\
&\overset{(b)}{=} n\epsilon_n + I(M;Y_1^{z_w}) + I\left(M;Y_{z_w+1}^{C}|Y_1^{z_w}\right) \\
&\overset{(c)}{\leq} n\epsilon_n + I\left(M;X_{z_w+1}^{C}\right) \\
&\overset{(d)}{\leq} n\epsilon_n + I\left(M;X_{z_w+1}^{z_w+z_r}\right) + I\left(M;X_{z_w+z_r+1}^{C}|X_{z_w+1}^{z_w+z_r}\right) \\
&\overset{(e)}{\leq} n\epsilon_n + H\left(X_{z_w+z_r+1}^{C}|X_{z_w+1}^{z_w+z_r}\right) \\
&\overset{(f)}{\leq} n\epsilon_n + C - z_w - z_r, \qquad (1)
\end{aligned}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Here, (a) follows from Fano's inequality. Inequalities (b) and (d) follow from the chain rule for mutual information. To obtain (c), we assume without loss of generality that Calvin jams first z_w links. Then, we get $I(M;Y_1^{z_w}) = 0$, as Calvin adds uniform random noise independent of Alice's transmissions. Also, $I\left(M;Y_{z_w+1}^{C}|Y_1^{z_w}\right) = I\left(M;Y_{z_w+1}^{C}\right)$ due to independence of added noise. Finally, we use the fact that for the set of uncorrupted links, we have $Y_{C\setminus Z_W} = X_{C\setminus Z_W}$, which gives $I\left(M;Y_{z_w+1}^{C}\right) = I\left(M;X_{z_w+1}^{C}\right)$. For getting (e), we use the fact that for any subset Z_R of links of size z_r, the secrecy requirement imposes that $I(M;X_{Z_R}) = 0$. Thus, $I\left(M;X_{z_w+1}^{z_w+z_r}\right) = 0$. In addition, we have $I\left(M;X_{z_w+z_r+1}^{C}|X_{z_w+1}^{z_w+z_r}\right) \leq H\left(X_{z_w+z_r+1}^{C}|X_{z_w+1}^{z_w+z_r}\right)$. Lastly, (f) follows from the fact $H\left(X_{z_w+z_r+1}^{C}|X_{z_w+1}^{z_w+z_r}\right) \leq H\left(X_{z_w+z_r+1}^{C}\right) \leq C - z_w - z_r$, where the second inequality is due to unit link capacities.

Achievability: Alice first appends $n(C - z_w - z_r)$ message symbols with nz_r uniform random key symbols to form $n(C - z_w)$ *super-message* symbols. Then, she uses the achievable scheme mentioned in the proof of Theorem 1 (case 1) composed of a $(C, C - z_w)$ Reed-Solomon code together with the pairwise hashing scheme. We require that the generator matrix of the Reed-Solomon code consists of a Cauchy matrix.

Now, Bob can locate the set Z_W of corrupted links using pairwise hashing and uses the Reed-Solomon code to decode the super-message symbols from the remaining links. Then, Bob separates the random keys and the message symbols from the super-message symbols, since the first $n(C - z_w - z_r)$ symbols of the super-message are the message symbols.

For secrecy, we show that Calvin cannot infer any information from the links he eavesdrops. We denote the set of random keys by k and the corresponding random variable by K. Further, let X_{Z_R} denote the links being eavesdropped. Consider the following set of inequalities.

$$\begin{aligned}
I(M;X_{Z_R}) &= H(X_{Z_R}) - H(X_{Z_R}|M) \\
&\overset{(g)}{\leq} nz_r - H(X_{Z_R}|M) \\
&\overset{(h)}{\leq} nz_r - H(X_{Z_R}|M) + H(X_{Z_R}|M,K) \\
&\overset{(i)}{=} nz_r - I(X_{Z_R};K|M) \\
&\overset{(j)}{=} nz_r - H(K|M) + H(K|M,X_{Z_R}) \\
&\overset{(k)}{=} nz_r - H(K) + H(K|M,X_{Z_R}) \\
&\overset{(l)}{\leq} H(K|M,X_{Z_R}), \qquad (2)
\end{aligned}$$

where (g) follows from from the fact that each link has unit capacity and Calvin can eavesdrop at most z_r links, (h) follows from the non-negativity of entropy, (i) and (j) follow from the definition of mutual information, (k) follows because keys are independent of the message, and (l) follows from the fact that the keys are uniform random, giving $H(K) = nz_r$. Now, in order to prove secrecy, we need to show that $H(K|M,X_{Z_R}) = 0$. In other words, one can decode the keys from X_{Z_R} and M. Let $G_{(X_{Z_R})}$ denote the rows of the Cauchy generator matrix corresponding to the symbols X_{Z_R}. Therefore, we have

$$X_{Z_R} = G_{(X_{Z_R})} \begin{bmatrix} M \\ K \end{bmatrix}.$$

To prove that $H\left(K|M, X_{Z_R}\right) = 0$, one needs to show that the following system of linear equations can be solved.

$$X_{Z_R} = \begin{bmatrix} G_{(X_{Z_R})} \\ I \mid O \end{bmatrix} \begin{bmatrix} M \\ K \end{bmatrix}, \tag{3}$$

where I denotes identity matrix of size $n(C-z_w-z_r)\times n(C-z_w-z_r)$, and O denotes zero matrix of size $n(C-z_w-z_r)\times nz_r$. First notice that $G_{(X_{Z_R})}$ is a Cauchy matrix since it is a sub-matrix of a Cauchy matrix. Then, using the property that any square sub-matrix of a Cauchy matrix is non-singular, it is straightforward to show that the matrix $\begin{bmatrix} G_{(X_{Z_R})} \\ I \mid O \end{bmatrix}$ is invertible. Therefore, the linear system (3) can be inverted, and we have $H\left(K|M, X_{Z_R}\right) = 0$.

2) Strong adversary Regime: Notice that even in the absence of secrecy, no positive rate is achievable in this regime. Adding the extra requirement of secrecy can only decrease the communication rate. Thus no communication at positive rate is possible in this regime.

B. Proof of Theorem 6

For the weak adversary case, the converse and achievability proofs follow from the same arguments as in the proof of Theorem 5 and is omitted for brevity.

For the strong adversary regime, the rate without the secrecy requirement is zero. This implies that no positive rate is possible when secrecy condition is added on top of reliability.

Appendix D
Proof for reliability with passive feedback

A. Proof of Theorem 7

Noting that the rate cannot exceed $C - z_w$ even with feedback (since Calvin can always inject random noise on z_w links). Therefore, to prove the claim of Theorem 7, it suffices to show the following:

- (a). $C - z_w$ is achievable whenever $z_r < C$ or $C > 2z_w$,
- (b). No positive rate is possible when $z_r = C$ and $C \leq 2z_w$.

1) Proof of (a): We prove the achievability of the rate $C - z_w$ by partitioning the parameter set $\mathcal{Z}^{add}_{pos,fb} = \{z_r < C\} \cup \{C > 2z_w\}$ into disjoint sets $\mathcal{Z}_1 = \{z_r < C\}$ and $\mathcal{Z}_2 = \{z_r = C\} \cap \{C > 2z_w\}$, and using different coding schemes in the two sets.

Achievability for $\mathcal{Z}_1$: The code operates over two rounds. In the first round, Alice uses an erasure code of length C capable of correcting upto z_w erasures. Upon observing the codewords received by Bob (through passive feedback), Alice computes random hashes of each of the C received codewords and sends these hashes on the links which are not corrupted in the first round.

Formally, we show that the rate $C - z_w$ is achievable (and hence, any smaller rate is also achievable). Alice first chooses a blocklength $n > \lceil \log_2 C \rceil$ and encodes an nR-bit message over $n + C\sqrt{n}$ time slots using a two-round scheme as follows. *Round 1:* In the first round, Alice uses n time slots to transmit using the following scheme. Alice treats m as R consecutive symbols $m_1, m_2, \ldots, m_R$ from a finite field $\mathbb{F}_{2^n}$ of size 2^n. Next, Alice encodes $(m_1, m_2, \ldots, m_R)$ to $X^{(1)} = (x_1^{(1)}, x_2^{(1)}, \ldots, x_C^{(1)})$ using a Reed-Solomon code capable of correcting upto z_w erasures and sends $x_i^{(1)}$ on the link L_i for each $i = 1, 2, \ldots, C$. These codewords are corrupted by Calvin and Bob receives $Y^{(1)} = (y_1^{(1)}, y_2^{(1)}, \ldots, y_C^{(1)})$. Alice also observes $Y^{(1)}$ causally using the passive feedback available to her. Based on her observation, Alice partitions $L_1, L_2, \ldots, L_C$ into two sets – $Z_\checkmark$ consisting of all links L_i where $x_i^{(1)} = y_i^{(1)}$ and $Z_\times$ consisting of all links L_i where $x_i \neq y_i$. Note that $Z_\times \subseteq Z_W \subsetneq \{L_1, L_2, \cdots, L_C\}$.

Round 2: In the second round, Alice uses the feedback seen from first round and transmits random hashes over $2C\sqrt{n}$ time slots using the following scheme. Alice picks C independent random keys $\rho_1, \rho_2, \ldots, \rho_C$ and computes hashes $h(y_1^{(1)}, \rho_1), h(y_2^{(1)}, \rho_2), \ \ldots, \ h(y_C^{(1)}, \rho_C)$, each of length $\lceil \sqrt{n} \rceil$ using the matrix hash scheme (See Appendix A). Next, Alice transmits the codeword $x_i^{(2)} = [h(y_1^{(1)}, \rho_1)\ h(y_2^{(1)}, \rho_2)\ \ldots h(y_C^{(1)}, \rho_C)\ \rho_1\ \rho_2\ \ldots\ \rho_C]$ on every link $L_i \in Z_\checkmark$ and a random length-$2C\sqrt{n}$ vector $x_i^{(2)}$ on every link $L_i \in Z_\times$.

Decoding: Bob first partitions the set of links into sets $\hat{Z}_\checkmark$ and $\hat{Z}_\times$ using the following classification.

- If Bob determines that the hash values and keys specified by $y_i^{(2)}$ are consistent with all the received codewords in the first round, *i.e.*, $Y^{(1)}$, he assigns L_i to $\hat{Z}_\checkmark$.
- Else, Bob assigns L_i to $\hat{Z}_\times$.

Finally, if the size of $\hat{Z}_\checkmark$ is at least as large as $C - z_w$, Bob uses the codewords $(x_i^{(1)} : L_i \in \hat{Z}_\checkmark)$ to decode the message. Else, he declares an error.

Analysis: Note that $\hat{Z}_\checkmark$ includes every link that is not corrupted by Calvin (and possibly some other links as well). Thus, $|\hat{Z}_\checkmark| \geq C - z_w$. Since the Reed-Solomon erasure correcting code can recover $X^{(1)}$ from any $C - z_w$ correct symbols out of $x_1^{(1)}, x_2^{(1)}, \ldots, x_C^{(1)}$, in order to prove that Bob can successfully decode m with a high probability, it is sufficient to show that $Z_\times \subseteq \hat{Z}_\times$ with a high probability. Without loss of generality, we show the above when $z_w < C$ (since zero rate is trivially achieved when $z_w = C$).

Let $L_s \in Z_\times$. Since $z_r < C$, there is at least one link L_t such that $y_t^{(1)}$ is observed by Bob (and hence by Alice), but not by Calvin. This implies that in the second round, even if Calvin knows ρ_t, he can only randomly guess a consistent replacement for $h(y_t^{(1)}, \rho_t)$. Thus,

$$\begin{aligned}
&\Pr\left(Z_\times \nsubseteq \hat{Z}_\times\right) \\
&\quad\leq \Pr\left(s \in \hat{Z}_\checkmark \middle| s \in Z_\times\right) \\
&\quad= \Pr\Big(y_s^{(2)} = [h(y_1^{(1)}, \hat{\rho}_1) \ldots h(y_C^{(1)}, \hat{\rho}_C)\ \hat{\rho}_1 \ldots \hat{\rho}_C] \\
&\qquad\qquad \text{for some } \hat{\rho}_1, \ldots, \hat{\rho}_C\Big) \\
&\quad\leq \Pr_{x_t^{(2)}, y_s^{(2)}}\left(\left(y_s^{(2)}\right)_{\lceil\sqrt{n}\rceil(s-1)+1}^{\lceil\sqrt{n}\rceil s} = h(y_t^{(1)}, \hat{\rho}_t) \middle| \hat{\rho}_t\right) \\
&\quad\leq 2^{-\sqrt{n}}.
\end{aligned}$$

In the above, the upper bound on the guessing probability follows from Lemma 2.

Achievability for $\mathcal{Z}_2$: In this parameter setting, we note that since $z_r = C$, $Z_W = Z_{RW}$ and $Z_{WO} = \emptyset$. Using the fact that $z_w < C/2$, Theorem 1, we can achieve a rate $C - z_{rw} - z_{wo}$ without using feedback.

2) Proof of (b): Next, we show that $z_r = C$ and Calvin controls more than half the links, Bob cannot distinguish between Alice and Calvin. Let $Z_1 = \{L_1, \ldots, L_{\lfloor C/2 \rfloor}\}$ and $Z_2 = \{L_{\lceil C/2 \rceil + 1}, \ldots, L_C\}$. Let $Z_E = \{L_{\lceil C/2 \rceil}\}$ if C is odd, and $\emptyset$ otherwise. Note that $|Z_1| = |Z_2| < z_w$.

For any message m and any code chose by Alice, Calvin's attack strategy is the following. First, Calvin adds a uniformly random noise sequence on any link in Z_E. Next, he selects a random message m' and chooses a set Z' uniformly at random from $\{Z_1, Z_2\}$. Finally, he uses Alice's coding strategy to encode the message m' over the links in Z'. Calvin can do this as $z_r = C$ and therefore, anything that is seen by Alice and Bob is also seen by Calvin.

Now, Bob is unable to reliably distinguish between following two cases:

- Alice's message is m and Calvin's message is m'.
- Alice's message is m' and Calvin's message is m.

Thus, the probability of error for Bob is at least $1/4$ if Alice's rate is non-zero. □

B. Proof of Theorem 8

From the point of view of the proof of Theorem 7, the overwrite jamming case differs from the additive one only in the respect that even on the links in Z_{WO}, Calvin knows the output (since he can replace it with anything of his choice). Thus the scheme from the proof of Theorem 7 works only if there is at least one link which is neither seen nor corrupted by Calvin.

The converse also follows similar arguments. If Calvin can see the output on all the links, he can follow a symmetrization strategy to confuse Bob if the rate is larger than $C - 2(z_{rw} + z_{wo})$. The idea is that if Calvin sees everything also seen by Bob and Alice, he can follow's Alice's coding scheme exactly but with a different message.

The proof is essentially the same as the proof of Theorem 7, and so we omit it here.

Appendix E
Causal Jamming with Passive Feedback and Secrecy

A. Proof of Theorem 9

Note that the converse arguments in this case are straightforward. When $z_w \geq z_r$, the rate cannot exceed $C - z_w$ since Calvin can always inject random noise on z_w links. When $z_r > z_w$, any set of z_r links cannot carry meaningful information due to secrecy requirement, which results in the rate $C - z_r$.

We present the proof of achievability for the regime $z_r \geq z_w$. The scheme for $z_w > z_r$ is analogous.

Encoding: The protocol operates over multiple rounds in four stages. Alice divides nR-bit message into NR number of symbols, where $N < n$ is such that $N|n$. Observe that each symbol is over the finite field $\mathbb{F}_q$ of size $q = 2^{n/N}$. Let $\tilde{z}_w$, $\tilde{z}_w \leq z_w$, be the number of links that Calvin chooses to corrupt in first N rounds. Let i_j be the round at which Calvin chooses to corrupt j-th of the z_w links that he can corrupt. Notice that $1 \leq i_1 \leq i_2 \leq \cdots \leq i_{\tilde{z}_w} \leq N$. In each round, Alice transmits encoded symbols over C links as described below.

Stage 1: The first stage is from rounds $1 \leq i \leq i_1$. In the first stage, in each round, Alice encodes $R = C - z_r$ message symbols (each over $\mathbb{F}_{2^{n/N}}$) together with z_r random keys (chosen uniformly and independently over $\mathbb{F}_{2^{n/N}}$). Let us denote the R message symbols transmitted during i-th round as $m_1^{(i)}, m_2^{(i)}, \cdots, m_R^{(i)}$, and the z_r random keys as $k_1^{(i)}, k_2^{(i)}, \cdots, k_{z_r}^{(i)}$. Then, alice generates C encoded symbols for the i-th round as

$$\begin{bmatrix} x_1^{(i)} \\ x_2^{(i)} \\ \vdots \\ x_C^{(i)} \end{bmatrix} = G \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k_{z_r}^{(i)} \end{bmatrix}, \tag{4}$$

where G is a $C \times C$ Cauchy matrix with each entry from $\mathbb{F}_{2^{n/N}}$.

Stage 2: The second stage is from rounds $i_1 + 1 \leq i \leq N$. Consider the case when Calvin has corrupted the j-th link ($1 \leq j \leq \tilde{z}_w$). Since Alice can overhear the transmissions till round i_j, she knows the links that Calvin has corrupted so far. We denote the set of corrupted links as $Z_w^{i_j} = \{l_1, \cdots, l_j\}$, and its complement as $\bar{Z}_w^{(i_j)}$. Let $y_{Z_w^{i_j}}^{(i-1)} = \{y_{l_1}^{(i-1)}, y_{l_2}^{(i-1)}, \cdots, y_{l_j}^{(i-1)}\}$ be the set of codewords received by Bob in round $i-1$ on the corrupted links. Then, the codewords transmitted in round i ($i_1 + 1 \leq i \leq N$), in stage 2, are given as

$$x_{\bar{Z}_w^{(i_j)}}^{(i)} = G_{\bar{Z}_w^{(i_j)}} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k_{z_r - j}^{(i)} \\ y_{Z_w^{(i_j)}}^{(i-1)} \end{bmatrix}, \tag{5}$$

$$x_{Z_w^{(i_j)}}^{(i)} = \begin{bmatrix} k_{z_r - j + 1}^{(i)} \\ \vdots \\ k_{z_r}^{(i)} \end{bmatrix}, \tag{6}$$

where $G_{\bar{Z}_w^{(i_j)}}$ is the sub-matrix of G formed by taking the rows of G corresponding to indices in the set $\bar{Z}_w^{(i_j)}$.

Stage 3: Since Alice overhears the symbols received by Bob in each round, Alice can easily determine $i_1, i_2, \cdots, i_{\tilde{z}_w}$. In stage 3, Alice sends pair of corrupted links and corrupted

indices, i.e., $x_l^{(N+1)} = \{i_1, l_1; i_2, l_2; \cdots; i_{\tilde{z}_w}, l_{\tilde{z}_w}\}$, on all of the links $1 \le l \le C$.

Stage 4: In the last stage, Alice computes a randomized hash of $y_l^{(1:N+1)}$ for each $1 \le l \le C$, as follows. First, Alice picks C independent random keys $\rho_1, \rho_2, \ldots, \rho_C$ and computes hashes $H = \{h(y_1^{(1:N+1)}, \rho_1), h(y_2^{(1:N+1)}, \rho_2), \ldots, h(y_C^{(1:N+1)}, \rho_C)\}$, each of length $\lceil \sqrt{n} \rceil$ using the matrix hash scheme (see appendix). Next, Alice transmits the hash H on every link $L_l \in L_{\bar{Z}_w^{(i_{\tilde{z}_w})}}$ and a random n-length vector $k_l^{(N+2)}$ on every link $L_l \in L_{Z_w^{(i_{\tilde{z}_w})}}$.

Decoding: The first phase of decoding works in the same way as in the scheme without secrecy. Bob first partitions the set of links into sets $\hat{Z}_\checkmark$ and $\hat{Z}_\times$ using the following classification.

- For each llink L_l, if Bob determines that the hash values and keys specified by H_l are consistent with all the received codewords on that link in the first three stages, *i.e.*, $y^{(1:N+1)}$, he assigns L_l to $\hat{Z}_\checkmark$.
- Else, Bob assigns L_l to $\hat{Z}_\times$.

From the links in $\hat{Z}_\checkmark$, Bob determines the corrupted links and the rounds from which Bob started corrupting the links, i.e., $\{i_1, l_1; i_2, l_2; \cdots; i_{\tilde{z}_w}, l_{\tilde{z}_w}\}$. Bob then decodes the codewords for each round starting from round 1 using the appropriate links for each round. In particular, he uses all the links for rounds $1 \le i \le i_1 - 1$, all the links except l_1 for rounds $i_1 + 1 \le i \le i_2 - 1$, and so on. If the set $\hat{Z}_\checkmark$ is empty, he declares an error.

Analysis for decoding: Note that $\hat{Z}_\checkmark$ includes every link that is not corrupted by Calvin. In order to prove that Bob can successfully decode m with a high probability, first, we need to show that $Z_w^{(i_{z_w})} = \hat{Z}_\times$ with a high probability. This proof is analogous to the case without secrecy.

Next, we need to show that Bob can decode for each round. In stage 1, till rounds $i_1 - 1$, no link is corrupted by Calvin. Thus, Bob can use (4) and invert G to decode the messages (and keys as well). In stage 2, let us consider the rounds from $i_j + 1 \le i \le i_{j+1} - 1$. In each of these rounds, notice that on uncorrupted links $\bar{Z}_w^{(i_j)}$, we have $y^{(i)}_{\bar{Z}_w^{(i_j)}} = x^{(i)}_{\bar{Z}_w^{(i_j)}}$. Thus, Bob can use (5) along with the received codewords in previous round on corrupted links $y^{(i-1)}_{Z_w^{(i_j)}}$ to get the following system of equations

$$\begin{bmatrix} x^{(i)}_{\bar{Z}_w^{(i_j)}} \\ y^{(i-1)}_{Z_w^{(i_j)}} \end{bmatrix} = \left[\begin{array}{c|c} G_{\bar{Z}_w^{(i_j)}} & \\ \hline \mathbf{0} & I_j \end{array}\right] \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k^{(i)}_{z_r - j} \\ y^{(i-1)}_{Z_w^{(i_j)}} \end{bmatrix}, \tag{7}$$

where $\mathbf{0}$ is a $j \times C - j$ zero matrix and I_j is a $j \times j$ identity matrix. Using the property of Cauchy matrix that any of its square sub-matrices is non-singular, it is easy to show that one can solve (7).

Remark: Note that in each of the rounds $i_1, i_2, \cdots, i_{\tilde{z}_w}$, Bob cannot decode the message symbols since Calvin corrupts the new link. Therefore, the number of symbols (messages plus keys) that can be correctly conveyed to Bob is $N - \tilde{z}_w \ge N - z_w \to N$ for large N.

Analysis for secrecy: We show that in any round, Calvin does not get any information about the message symbols. In the first stage, in round i, $1 \le i \le i_1$, Calvin gets the following system of equations on the links Z_r that he can observe:

$$x^{(i)}_{Z_r} = G_{Z_r} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k_{z_r}^{(i)} \end{bmatrix}, \tag{8}$$

where G_{Z_r} is the sub-matrix of G rows corresponding to links in Z_w. Using the properties of Cauchy matrix, we can prove that $I\left(M; x^{(i)}_{Z_r}\right) = 0$ using the same steps as in the case without passive feedback.

Next, we prove secrecy for every round i, $i_1 + 1 \le i \le N$, in stage 2. Consider the case that Calvin has corrupted j links, $1 \le j \le \tilde{z}_w$. Let $\tilde{z}_{rw}^{(j)}$ be the number of corrupted links that Calvin can also eavesdrop, and $\tilde{z}_{wo}^{(j)}$ be the remaining corrupted links ($\tilde{z}_{rw}^{(j)} + \tilde{z}_{wo}^{(j)} = j$). Note that Calvin observes (left hand side of) the following system of equations:

$$\begin{bmatrix} x^{(i)}_{z_r} \\ y^{(i-1)}_{\tilde{z}_{rw}^{(j)}} \end{bmatrix} = \left[\begin{array}{c|c} G_{z_r} & \\ \hline \mathbf{0} & I_{\tilde{z}_{rw}^{(j)}} \end{array}\right] \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k^{(i)}_{z_r - j} \\ y^{(i-1)}_{\tilde{z}_{wo}^{(j)}} \\ y^{(i-1)}_{\tilde{z}_{rw}^{(j)}} \end{bmatrix}, \tag{9}$$

where $\mathbf{0}$ is a $j \times \tilde{z}_{wo}^{(j)}$ zero matrix, and $I_{\tilde{z}_{rw}^{(j)}}$ is $\tilde{z}_{rw}^{(j)} \times \tilde{z}_{rw}^{(j)}$ identity matrix. Out of the eavesdropped codewords $x^{(i)}_{z_r}$, the ones on the read-write links are random keys (12). Thus, in round i, the number of codewords containing messages that are observed by Calvin is $z_{ro} + z_{rw} - \tilde{z}_{wo}^{(j)} = z_r - \tilde{z}_{wo}^{(j)}$.

Now, observe that Alice mixes $z_{ro} - j$ explicit random keys. Out of the randomness generated over j corrupted links by Calvin $Z_w^{(i_j)}$ using previous round codewords, Calvin knows $y^{(i-1)}_{\tilde{z}_{rw}^{(j)}}$ due to his eavesdropping power on those links. Since he cannot eavesdrop on remaining of the j links, $y^{(i-1)}_{\tilde{z}_{wo}^{(j)}}$ act as random keys. Thus, the total number of random keys used by Alice are $(z_{ro} - j) + (j - \tilde{z}_{rw}^{(j)}) = z_{ro} - \tilde{z}_{rw}^{(j)}$. Hence, the number of keys equals the number of observed codewords. We can prove that no information is leaked using the properties of Cauchy matrix, using the same technique as in the case without passive feedback.

B. Proof of Theorem 10

The flavor of the scheme and the proof remains the same as above. The key difference is the following. In stage 2, when Calvin corrupts a link, Alice stops using that link and, on the contrary to the additive noise case, she does not initially reduce the number of explicit keys. After Calvin corrupts z_{wo} links, for each additional corrupted link starting with $(z_{wo}+1)$-th link, Alice reduces the number of explicit keys by one. Besides, she also stops using that link. Therefore, essentially, Alice does not send any data on (up to) z_w links, and on remaining links she mixes message symbols with (at least) z_{ro} random keys for secrecy.

We first present achievability scheme.

Encoding: The protocol operates over multiple rounds in four stages. Alice divides nR-bit message into NR number of symbols, where $N < n$ is such that $N|n$. Observe that each symbol is over the finite field $\mathbb{F}_q$ of size $q = 2^{n/N}$. Let $\tilde{z}_w$, $\tilde{z}_w \leq z_w$, be the number of links that Calvin chooses to corrupt in first N rounds. Let i_j be the round at which Calvin chooses to corrupt j-th of the z_w links that he can corrupt. Notice that $1 \leq i_1 \leq i_2 \leq \cdots \leq i_{\tilde{z}_w} \leq N$. In each round, Alice transmits encoded symbols over C links as described below.

Stage 1: The first stage is from rounds $1 \leq i \leq i_1$. In the first stage, in each round, Alice enodes $R = C - z_{ro} - z_{wo} - z_{rw}$ message symbols (each over $\mathbb{F}_{2^{n/N}}$) together with z_r random keys (chosen uniformly and independently over $\mathbb{F}_{2^{n/N}}$). Let us denote the R message symbols transmitted during i-th round as $m_1^{(i)}, m_2^{(i)}, \cdots, m_R^{(i)}$, and the z_r random keys as $k_1^{(i)}, k_2^{(i)}, \cdots, k_{z_r}^{(i)}$. Then, Alice generates C encoded symbols for the i-th round as follows.

$$\begin{bmatrix} x_1^{(i)} \\ x_2^{(i)} \\ \vdots \\ x_C^{(i)} \end{bmatrix} = G \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k_{z_r}^{(i)} \end{bmatrix}, \tag{10}$$

where G is a $C \times C - z_{wo}$ Cauchy matrix with each entry from $\mathbb{F}_{2^{n/N}}$.

Stage 2: The second stage is from rounds $i_1 + 1 \leq i \leq N$. Consider the case when Calvin has corrupted the j-th link ($1 \leq j \leq \tilde{z}_w$). Since Alice can overhear the transmissions till round i_j, she knows the links that Calvin has corrupted so far. Once Calvin corrupts a link, Alice starts sending random symbols on that link from the next round. Essentially, Alice stops using the corrupted links for any meaningful transmission. If $j \leq z_{wo}$, Alice keeps mixing z_r keys, else she reduces the number of keys by one for each corrupted link.

To describe this formally, we denote the set of j links that have been corrupted up to round i_j as $Z_w^{i_j} = \{l_1, \cdots, l_j\}$, and its complement as $\bar{Z}_w^{(i_j)}$. The codewords transmitted in round i ($i_1 + 1 \leq i \leq N$), in stage 2, are given as

$$x^{(i)}_{\bar{Z}_w^{(i_j)}} = G_{\bar{Z}_w^{(i_j)}} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k^{(i)}_{z_r-(j-z_{wo})^+} \end{bmatrix}, \tag{11}$$

where $G_{\bar{Z}_w^{(i_j)}}$ is the sub-matrix of G formed by taking the rows of G corresponding to indices in the set $\bar{Z}_w^{(i_j)}$ and first $R + z_r - (j - z_{wo})^+$ columns, and

$$x^{(i)}_{Z_w^{(i_j)}} = \begin{bmatrix} k^{(i)}_{z_r-(j-z_{wo})^+ +1} \\ \vdots \\ k^{(i)}_{z_r-(j-z_{wo})^+ +j} \end{bmatrix}. \tag{12}$$

Stage 3: Since Alice overhears the symbols received by Bob in each round, Alice can easily determine $i_1, i_2, \cdots, i_{\tilde{z}_w}$. In stage 3, Alice sends pair of corrupted links and corrupted indices, i.e., $x_l^{(N+1)} = \{i_1, l_1; i_2, l_2; \cdots; i_{\tilde{z}_w}, l_{\tilde{z}_w}\}$, on all of the links $1 \leq l \leq C$.

Stage 4: The last stage is similar to the second stage in the scheme for only reliability. The purpose of this stage is to allow Bob to determine the corrupted links and the corresponding rounds. In this stage, Alice computes a randomized hash of the symbols received by Bob in the previous N rounds, i.e., $y_l^{(1:N+1)}$, for each link $1 \leq l \leq C$, as follows. First, Alice picks C independent random keys $\rho_1, \rho_2, \ldots, \rho_C$ and computes hashes $H_l = h(y_l^{(1:N+1)}, \rho_l)$, $1 \leq l \leq C$, each of length $\lceil \sqrt{n} \rceil$ using the matrix hash scheme (see appendix). Next, Alice transmits the hash H on every uncorrupted link $L_l \in L_{\bar{Z}_w^{(i_{\tilde{z}_w})}}$ and a random $C\lceil \sqrt{n} \rceil$-length vector $k_l^{(N+2)}$ on every corrupted link $L_l \in L_{Z_w^{(i_{\tilde{z}_w})}}$.

Decoding: The first phase of decoding works in the same way as in the scheme without secrecy. Bob first partitions the set of links into sets $\hat{Z}_\checkmark$ and $\hat{Z}_\times$ using the following classification.

- For each llink L_l, if Bob determines that the hash values and keys specified by H_l are consistent with all the received codewords on that link in the first three stages, *i.e.*, $y^{(1:N+1)}$, he assigns L_l to $\hat{Z}_\checkmark$.
- Else, Bob assigns L_l to $\hat{Z}_\times$.

From the links in $\hat{Z}_\checkmark$, Bob determines the corrupted links and the corresponding rounds from which Bob started corrupting the links, i.e., $\{i_1, l_1; i_2, l_2; \cdots; i_{\tilde{z}_w}, l_{\tilde{z}_w}\}$. Bob then decodes the codewords for each round starting from round 1 using the appropriate links for that round. In particular, he uses all the links for rounds $1 \leq i \leq i_1 - 1$, all the links except l_1 for rounds $i_1 + 1 \leq i \leq i_2 - 1$, and so on. If the set $\hat{Z}_\checkmark$ is empty, he declares an error.

Analysis for decoding: Note that $\hat{Z}_\checkmark$ includes every link that is not corrupted by Calvin. In order to prove that Bob can successfully decode m with a high probability, first, we need to show that $Z_w^{(i_{z_w})} = \hat{Z}_\times$ with a high probability. This proof is analogous to the case without secrecy.

Next, we need to show that Bob can decode for each round. In stage 1, till rounds $i_1 - 1$, no link is corrupted by Calvin. Thus, Bob can use (10) and use any $C - z_{wo}$ rows of G to decode the messages (and keys as well).[9]

In stage 2, let us consider the rounds from $i_j + 1 \leq i \leq i_{j+1} - 1$. In each of these rounds, notice that on uncorrupted links $\bar{Z}_w^{(i_j)}$, we have $y^{(i)}_{\bar{Z}_w^{(i_j)}} = x^{(i)}_{\bar{Z}_w^{(i_j)}}$. Thus, Bob can use (15) to get the following system of equations

$$x^{(i)}_{\bar{Z}_w^{(i_j)}} = G_{\bar{Z}_w^{(i_j)}} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k^{(i)}_{z_r-(j-z_{wo})^+} \end{bmatrix}. \tag{13}$$

Observe that the number of rows of $G_{\bar{Z}_w^{(i_j)}}$ is $C-j$, while the number of columns is $R + z_r - (j - z_{wo})^+ = C - z_{wo} - (j - z_{wo})^+$. If $j \leq z_{wo}$, Bob can consider any $C - z_{wo}$ rows of the Cauchy matrix $G_{\bar{Z}_w^{(i_j)}}$ to decode for the message and key symbols. If $j > z_{wo}$, $G_{\bar{Z}_w^{(i_j)}}$ is square and it is non-singular being a Cauchy matrix.

Remark: Note that in each of the rounds $i_1, i_2, \cdots, i_{\tilde{z}_w}$, Bob cannot decode the message symbols since Calvin corrupts the new link. Therefore, the number of symbols (messages plus keys) that can be correctly conveyed to Bob is $N - \tilde{z}_w \geq N - z_w \to N$ for large N.

Analysis for secrecy: We show that in any round, Calvin does not get any information about the message symbols. In the first stage, in round i, $1 \leq i \leq i_1$, Calvin gets the following system of equations on the links Z_r that he can observe:

$$x^{(i)}_{Z_r} = G_{Z_r} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k_{z_r}^{(i)} \end{bmatrix}, \tag{14}$$

where G_{Z_r} is the sub-matrix of G rows corresponding to links in Z_w. Using the properties of Cauchy matrix, we can prove that $I\left(M; x^{(i)}_{Z_r}\right) = 0$ using the same steps as in the case for secrecy without passive feedback.

Next, we prove secrecy for every round i, $i_1 + 1 \leq i \leq N$, in stage 2. Consider the case that Calvin has corrupted j links, $1 \leq j \leq \tilde{z}_w$. Let $\tilde{z}^{(j)}_{rw}$ be the number of corrupted links that Calvin can also eavesdrop, and $\tilde{z}^{(j)}_{wo}$ be the remaining corrupted links ($\tilde{z}^{(j)}_{rw} + \tilde{z}^{(j)}_{wo} = j$). Note that Calvin observes (left hand side of) the following system of equations:

$$\begin{bmatrix} x^{(i)}_{z_{rw}-\tilde{z}^{(j)}_{rw}} \\ x^{(i)}_{z_{ro}} \end{bmatrix} = G_{z_{rw}-\tilde{z}^{(j)}_{rw}+z_{ro}} \begin{bmatrix} m_1^{(i)} \\ \vdots \\ m_R^{(i)} \\ k_1^{(i)} \\ \vdots \\ k^{(i)}_{z_r-(j-z_{wo})^+} \end{bmatrix}, \tag{15}$$

$$x^{(i)}_{\tilde{z}^{(j)}_{rw}} = \begin{bmatrix} k^{(i)}_{z_r-(j-z_{wo})^+ +1} \\ \vdots \\ k^{(i)}_{z_r-(j-z_{wo})^+ +\tilde{z}^{(j)}_{rw}} \end{bmatrix}, \tag{16}$$

On $\tilde{z}^{(j)}_{rw}$ links, Calvin observes random keys. Thus, we need to worry about the remaining of the $z_r - \tilde{z}^{(j)}_{rw}$ links that he eavesdrops. The number of random key symbols mixed with message symbols is $z_r - (j - z_{wo})^+$. If $j \leq z_{wo}$, the number of mixed keys is z_r, while if $j > z_{wo}$, the number of mixed keys is $z_r - (j - z_{wo}) = z_r - \tilde{z}^{(j)}_{rw} - \tilde{z}^{(j)}_{wo} + z_{wo}$. Since $\tilde{z}^{(j)}_{wo} \leq z_{wo}$, it is easy to see that the number of mixed keys is greater than equal to the number of eavesdropped symbols involving messages. Using the properties of Cauchy matrix, one can easily prove that the secrecy requirement is satisfied.

Converse: Consider a strategy for Calvin wherein he overwrites zero symbols on the z_{wo} links that he can only corrupt. He eavesdrops all the z_r links of his choice. We consider that the communication is over multiple rounds, say t number of rounds.

$$\begin{aligned} H(M) &= H\left(M|Y^{(1:n)}\right) + I\left(M; Y^{(1:n)}\right) \\ &\overset{(a)}{\leq} n\epsilon_n + I\left(M; Y^{(1:n)}\right) \\ &\overset{(b)}{=} n\epsilon_n + I\left(M; Y^{(1:n)}_{z_{ro}+z_{rw}}\right) + I\left(M; Y^{(1:n)}_{z_{wo}} | Y^{(1:n)}_{z_{ro}+z_{rw}}\right) \\ &\quad + I\left(M; Y^{(1:n)}_{C-z_{wo}-z_{ro}-z_{rw}} | Y^{(1:n)}_{z_{wo}+z_{ro}+z_{rw}}\right) \\ &\overset{(c)}{=} n\epsilon_n + I\left(M; Y^{(1:n)}_{C-z_{wo}-z_{ro}-z_{rw}} | Y^{(1:n)}_{z_{ro}+z_{wo}+z_{rw}}\right) \\ &\leq n\epsilon_n + H\left(Y^{(1:n)}_{C-z_{wo}-z_{ro}-z_{rw}}\right) \\ &\overset{(d)}{\leq} n\epsilon_n + n(C - z_{wo} - z_{ro} - z_{rw}), \end{aligned}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Here, (a) follows from Fano's inequality, (b) follows from the chain rule of mutual information. To obtain (c), first note that $I\left(M; Y^{(1:n)}_{z_{ro}+z_{rw}}\right) \leq I\left(M; X^{(1:n)}_{z_{ro}+z_{rw}}\right)$ by data processing inequality. But, for secrecy, we need $I\left(M; X^{(1:n)}_{z_{ro}+z_{rw}}\right) = 0$. Also, $I\left(M; Y^{(1:n)}_{z_{wo}} | Y^{(1:n)}_{z_{ro}+z_{rw}}\right) = 0$ since $Y^{(1:n)}_{z_{wo}} = 0$ due to Calvin's attack strategy. Finally, (d) follows from unit link capacities.

[9]Here, we use the property of a Cauchy matrix that any of its square sub-matrices is non-singular.